

GENERALIZED PROJECTIONS IN \mathbb{Z}_n

ANIL KHAIRNAR AND B. N. WAPHARE

Abstract: We consider the ring \mathbb{Z}_n (integers modulo n) with the partial order ' \leq ' given by ' $a \leq b$ if either $a = b$ or $a \equiv ab \pmod{n}$ '. In this paper, we obtain necessary and sufficient conditions for the poset (\mathbb{Z}_n, \leq) to be a lattice.

Keywords: generalized projections, regular elements, nilpotent elements.

1. INTRODUCTION

An element a in a commutative ring R is said to be a *generalized projection* if $a^k = a$ for some $k \in \mathbb{N}$ with $k \geq 2$ (see [1]); an element a is called a *regular element* if $a = aba (= a^2b)$ for some element b in the ring. It is proved by László Tóth [2] that in \mathbb{Z}_n , an element is a generalized projection if and only if it is regular; in-fact the following result is proved.

Theorem 1.1 ([2], Theorem 1). *Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i . For an integer $a \geq 1$, the following assertions are equivalent:*

- i) a is regular \pmod{n} ; ii) for every $i \in \{1, 2, \dots, k\}$, either $p_i^{\alpha_i} | a$ or $p_i \nmid a$;
- iii) $\gcd(a, n) = \gcd(a^2, n)$; iv) $\gcd(a, n) | n$ and $\gcd(\gcd(a, n), \frac{n}{\gcd(a, n)}) = 1$;
- v) $a^{\varphi(n)+1} \equiv a \pmod{n}$; vi) there exists an integer $m \geq 1$ such that $a^{m+1} \equiv a \pmod{n}$.

We denote by $GP(\mathbb{Z}_n)$, the set of generalized projections (i.e. the set of regular elements) and $P(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid a^2 = a\}$, the set of projections in \mathbb{Z}_n . Let R be a commutative ring, the relation ' \leq ' defined by: for $a, b \in R$, ' $a \leq b$ if and only if either $a = b$ or $a = ab$ ' is a partial order on R (see [1]). In particular, (\mathbb{Z}_n, \leq) is a poset with the smallest element 0 and the largest element 1. It is known that $(P(\mathbb{Z}_n), \leq)$ is a lattice. However, Khairnar and Waphare [1] proved that for any finite commutative ring R , $(GP(R), \leq)$ is a lattice, hence in particular, $(GP(\mathbb{Z}_n), \leq)$ is a lattice for every n . Whenever n is a square-free integer, we get that $GP(\mathbb{Z}_n) = \mathbb{Z}_n$. In general, (\mathbb{Z}_n, \leq) is not a lattice, for example (\mathbb{Z}_9, \leq) (see Figure 2). In this paper, we give a necessary and sufficient conditions for the poset (\mathbb{Z}_n, \leq) to be a lattice.

We denote by $U(\mathbb{Z}_n)$, the set of units in \mathbb{Z}_n and $N(\mathbb{Z}_n)$, the set of nilpotents in \mathbb{Z}_n . In the following remark, we list observations required in a sequel.

Remark 1.2. Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i , and let $a \in \mathbb{Z}_n$. Then,

- (i) $a \in U(\mathbb{Z}_n)$ if and only if $a \equiv \text{unit} \pmod{p_i}$ for all $i \in \{1, 2, \dots, k\}$.
- (ii) $a \in N(\mathbb{Z}_n)$ if and only if $a \equiv \text{zero} \pmod{p_i}$ for all $i \in \{1, 2, \dots, k\}$.
- (iii) $a \in GP(\mathbb{Z}_n)$ if and only if $a \equiv \text{zero or unit} \pmod{p_i^{\alpha_i}}$ for all $i \in \{1, 2, \dots, k\}$.

2. UPPER COVERING PROJECTION AND LOWER COVERING PROJECTION

In a poset (P, \leq) , $a < b$ denotes $a \leq b$ with $a \neq b$. We say that b is an *upper cover* of a or a is a *lower cover* of b (denoted by $a < b$), if $a < b$ and there is no $c \in P$ such that $a < c < b$.

The following theorem gives an existence of the unique lower cover and the unique upper cover of any element $a \in GP(R) \setminus P(R)$ in the poset $GP(R)$.

Theorem 2.1 ([1], Theorem 2.7). *Let R be a finite commutative ring. If $a \in GP(R) \setminus P(R)$, then there exist a unique $a_u \in GP(R)$ and a unique $a_l \in GP(R)$ such that $a_l < a < a_u$. Further, these unique elements are projections and for $b \in GP(R)$, $a < b$ if and only if $a_u \leq b$; and $b < a$ if and only if $b \leq a_l$.*

With notations as in Theorem 2.1, the unique projection a_l is called the *lower covering projection* of a and the unique projection a_u is called the *upper covering projection* of a . If a is a projection, then we assume that the lower covering projection of a and the upper covering projection of a is a itself.

Theorem 2.1 gives an existence of the upper covering projection and the lower covering projection of any element in $GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$. In this section, we determine the upper covering projection and the lower covering projection of elements in $GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$.

The following lemma gives the conditions for strict comparability of a projection and a generalized projection.

Lemma 2.2. *Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i . Let $a \in GP(\mathbb{Z}_n)$ and $e, f \in P(\mathbb{Z}_n) \setminus \{1\}$. Then,*

- (1) $a < e$ if and only if for $i \in \{1, 2, \dots, k\}$, $e \equiv 0 \pmod{p_i^{\alpha_i}}$ implies that $a \equiv 0 \pmod{p_i^{\alpha_i}}$.
- (2) $f < a$ if and only if for $j \in \{1, 2, \dots, k\}$, $f \not\equiv 0 \pmod{p_j^{\alpha_j}}$ implies that $a \equiv 1 \pmod{p_j^{\alpha_j}}$.

Proof. (1) Let $a < e$ and $i \in \{1, 2, \dots, k\}$ be such that $e \equiv 0 \pmod{p_i^{\alpha_i}}$. Then $a(1 - e) \equiv 0 \pmod{n}$ and $1 - e \not\equiv 0 \pmod{p_i^{\alpha_i}}$. Therefore $a \equiv 0 \pmod{p_i^{\alpha_i}}$. Conversely, suppose that for $i \in \{1, 2, \dots, k\}$, $e \equiv 0 \pmod{p_i^{\alpha_i}}$ implies that $a \equiv 0 \pmod{p_i^{\alpha_i}}$. Then $a(1 - e) \equiv 0 \pmod{n}$. Thus $a < e$.

(2) Let $f < a$ and $j \in \{1, 2, \dots, k\}$ be such that $f \not\equiv 0 \pmod{p_j^{\alpha_j}}$. Then $1 - a \equiv 0 \pmod{p_j^{\alpha_j}}$. Therefore $a \equiv 1 \pmod{p_j^{\alpha_j}}$. Conversely, suppose that for $j \in \{1, 2, \dots, k\}$, $f \not\equiv 0 \pmod{p_j^{\alpha_j}}$ implies that $a \equiv 1 \pmod{p_j^{\alpha_j}}$. This gives $f(1 - a) \equiv 0 \pmod{n}$. Thus $f < a$. \square

Remark 2.3 ([1], Remark 3). Let $a \in GP(\mathbb{Z}_n)$. Suppose $k \geq 2$ be the smallest integer such that $a^k = a$. Then $(a^{k-1})^2 = a^{2k-2} = a^k a^{k-2} = a a^{k-2} = a^{k-1}$. Therefore $a^{k-1} \in P(\mathbb{Z}_n)$, and $a^{k-1} = a_u$. Clearly, $a \leq a_u$; and $a = a_u$ if and only if $a \in P(\mathbb{Z}_n)$.

For any $a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$ the following theorem gives a construction for a_u .

Theorem 2.4. *Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i , and $a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$. If $a \in U(\mathbb{Z}_n)$, then $a_u = 1$. If $a \notin U(\mathbb{Z}_n)$, then $a_u = b^{\varphi(\frac{n}{b})}$ where*

$$b = \prod_{j=1}^k p_j^{\alpha_j} \quad a \equiv 0 \pmod{p_j^{\alpha_j}}$$

Proof. Let $a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$. If $a \in U(\mathbb{Z}_n)$ then by Remark 2.3, $a_u = 1$. Suppose $a \notin U(\mathbb{Z}_n)$. By Remark 1.2, there exists $j \in \{1, 2, \dots, k\}$ such that $a \equiv 0 \pmod{p_j^{\alpha_j}}$, and

$a \equiv 0$ or unit (mod $p_i^{\alpha_i}$) for all $i \neq j$. Let $b = \prod_{j=1}^k p_j^{\alpha_j}$ and $a_u = b^{\varphi(\frac{n}{b})}$. Then $a \equiv 0 \pmod{p_j^{\alpha_j}}$

$a_u \in P(\mathbb{Z}_n)$ and by Lemma 2.2, $a \leq a_u$. Let $e \in P(\mathbb{Z}_n)$ be such that $a < e$. If $e = 1$, then $a_u \leq e$. Suppose $e \neq 1$. Again by Lemma 2.2, for $i \in \{1, 2, \dots, k\}$, $e \equiv 0 \pmod{p_i^{\alpha_i}}$ implies that $a \equiv 0 \pmod{p_i^{\alpha_i}}$. Hence, for $i \in \{1, 2, \dots, k\}$, $e \equiv 0 \pmod{p_i^{\alpha_i}}$ implies that $a_u \equiv 0 \pmod{p_i^{\alpha_i}}$. Thus $a_u \leq e$. \square

For any $a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$ the following theorem gives a construction for a_l .

Theorem 2.5. Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i , and

$a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$. Then $a_l = b^{\varphi(\frac{n}{b})}$ where $b = \prod_{j=1}^k p_j^{\alpha_j}$ and $a \not\equiv 1 \pmod{p_j^{\alpha_j}}$.

Proof. Let $a \in GP(\mathbb{Z}_n) \setminus P(\mathbb{Z}_n)$. If $a \equiv 1 \pmod{p_j^{\alpha_j}}$ for all $j \in \{1, 2, \dots, k\}$ then $a - 1 \equiv 0 \pmod{n}$. Hence $a = 1 \in P(\mathbb{Z}_n)$, a contradiction. Therefore there exists $j \in \{1, 2, \dots, k\}$ such that $a \not\equiv 1 \pmod{p_j^{\alpha_j}}$. Let $b = \prod_{j=1}^k p_j^{\alpha_j}$ and $a_l = b^{\varphi(\frac{n}{b})}$. We prove that $a_l \leq a$. Let $i \in \{1, 2, \dots, k\}$ be such that $a_l \not\equiv 0 \pmod{p_i^{\alpha_i}}$. Then $b \not\equiv 0 \pmod{p_i^{\alpha_i}}$ and hence $a \equiv 1 \pmod{p_i^{\alpha_i}}$. This yields, $a_l(a - 1) \equiv 0 \pmod{n}$. Therefore $a_l \leq a$. Let $f \in P(\mathbb{Z}_n)$ be such that $f < a$, and $j \in \{1, 2, \dots, k\}$ be such that $f \not\equiv 0 \pmod{p_j^{\alpha_j}}$. Then by Lemma 2.2, we get $a \equiv 1 \pmod{p_j^{\alpha_j}}$. Consequently, $b \not\equiv 0 \pmod{p_j^{\alpha_j}}$ and hence $a_l \not\equiv 0 \pmod{p_j^{\alpha_j}}$. This implies that $a_l \equiv 1 \pmod{p_j^{\alpha_j}}$. Therefore $f(1 - a_l) \equiv 0 \pmod{n}$. Thus $f \leq a_l$. \square

Let P be a poset and $a, b \in P$. The *join* of a and b , denoted by $a \vee b$, is defined as $a \vee b = \sup \{a, b\}$. The *meet* of a and b , denoted by $a \wedge b$, is defined as $a \wedge b = \inf \{a, b\}$.

We conclude this section with the following examples.

In the following example, $n \in \mathbb{N}$ is not square-free but the poset \mathbb{Z}_n is a lattice.

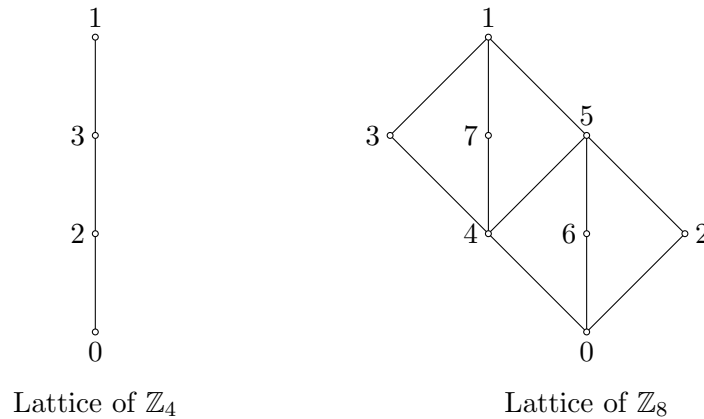


FIGURE 1

Example 2.6. Consider the ring \mathbb{Z}_4 . Then $GP(\mathbb{Z}_4) = \{0, 1, 3\}$ and $N(\mathbb{Z}_4) = \{0, 2\}$. Note that 4 is not square-free but the poset \mathbb{Z}_4 is a lattice (see Figure 1). Also, the nilpotent element 2 possess unique upper cover.

Example 2.7. Consider the ring \mathbb{Z}_8 . Then $GP(\mathbb{Z}_8) = \{0, 1, 3, 5, 7\}$ and $N(\mathbb{Z}_8) = \{0, 2, 4, 6\}$. Note that 8 is not square-free but the poset \mathbb{Z}_8 is a lattice (see Figure 1). Also, each of 2 and 6 possess unique upper covers but 4 does not possess unique upper cover.

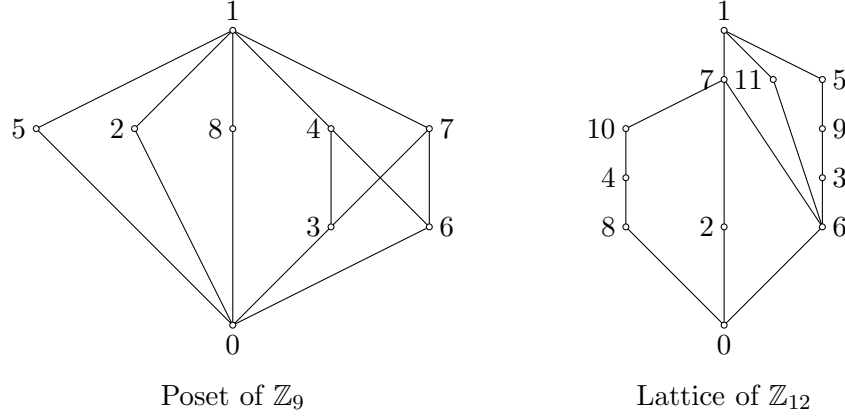


FIGURE 2

In the following example, the poset \mathbb{Z}_n is not a lattice. Also, none of the nilpotent elements possess unique upper cover.

Example 2.8. Consider the ring \mathbb{Z}_9 . Then $GP(\mathbb{Z}_9) = \{0, 1, 2, 4, 5, 7, 8\}$ and $N(\mathbb{Z}_9) = \{0, 3, 6\}$. By Figure 2, the poset \mathbb{Z}_9 is not a lattice. Note that $3 \vee 6$ and $4 \wedge 7$ do not exist. Also, each of 3 and 6 do not possess unique upper covers and each of 4 and 7 do not possess unique lower covers.

In the following example, n is not square-free but the poset \mathbb{Z}_n is a lattice.

Example 2.9. Consider the ring \mathbb{Z}_{12} . Then $GP(\mathbb{Z}_{12}) = \{0, 1, 3, 4, 5, 7, 8, 9, 11\}$ and $N(\mathbb{Z}_{12}) = \{0, 6\}$. Note that 12 is not square-free but the poset \mathbb{Z}_{12} is a lattice (see Figure 2). Observe that, the nilpotent element 6 does not possess an unique upper cover.

In the next section, we give a necessary and sufficient condition for the existence of supremum and infimum of any two elements of the poset \mathbb{Z}_n .

3. EXISTENCE OF $a \vee b$ AND $a \wedge b$ FOR $a, b \in \mathbb{Z}_n$

For $x \in \mathbb{Z}_n$, the ideal generated by x is denoted by (x) .

The following theorem characterizes the existence of $a \vee b$ for $a, b \in \mathbb{Z}_n$.

Theorem 3.1. Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i . Let $a, b \in \mathbb{Z}_n$ be incomparable and $d = \gcd(\gcd(a, b), n)$. Then, $a \vee b$ exists if and only if the coset $(\frac{n}{d}) + 1$ has the smallest element.

Proof. For each $i \in \{1, 2, \dots, k\}$, let $\beta_i, \gamma_i \in \mathbb{W} = \mathbb{N} \cup \{0\}$ be the largest powers of prime p_i such that $a \equiv 0 \pmod{p_i^{\beta_i}}$ and $b \equiv 0 \pmod{p_i^{\gamma_i}}$ respectively. Let $f_i = \max\{(\alpha_i - \beta_i), (\alpha_i - \gamma_i), 0\}$ and $m = \prod_{i=1}^k p_i^{f_i}$. Then $m = \frac{n}{d}$. Let $c \in \mathbb{Z}_n$ and for each $i \in \{1, 2, \dots, k\}$, let $t_i \in \mathbb{N}$ be the largest powers of prime p_i such that $c \equiv 1 \pmod{p_i^{t_i}}$. Then, $a < c$ and $b < c$, if and only if

$a(c-1) \equiv 0 \pmod{n}$ and $b(c-1) \equiv 0 \pmod{n}$, if and only if $t_i \geq (\alpha_i - \beta_i), (\alpha_i - \gamma_i)$ for all i , if and only if $c-1 \in (\frac{n}{d})$, if and only if $c \in (\frac{n}{d}) + 1$.

Suppose $a \vee b$ exists. Since a and b are incomparable, we have $a < a \vee b$ and $b < a \vee b$. This yields $a \vee b \in (\frac{n}{d}) + 1$. Let $x \in (\frac{n}{d}) + 1$. Then $a < x$ and $b < x$. Therefore $a \vee b \leq x$. Thus $a \vee b$ is the smallest element of the coset $(\frac{n}{d}) + 1$. Conversely, suppose that the coset $(\frac{n}{d}) + 1$ has the smallest element, say $e \in (\frac{n}{d}) + 1$. This yields $a < e$ and $b < e$. We claim that $a \vee b = e$. Let $f \in \mathbb{Z}_n$ be such that $a < f$ and $b < f$. Then $f \in (\frac{n}{d}) + 1$. Therefore $e \leq f$. Thus $a \vee b = e$. \square

From the proof of Theorem 3.1, it is clear that, if $a \vee b$ exists, then $a \vee b$ is the least element of the coset $(\frac{n}{d}) + 1$. Also, if the coset $(\frac{n}{d}) + 1$ has the smallest element e , then $a \vee b = e$.

The following corollary is an immediate consequence of Theorem 3.1.

Corollary 3.2. *Let $n \in \mathbb{N}$, $n > 1$ and $S = \{d \in \mathbb{N} \mid d = \gcd(\gcd(a, b), n)\}$, for some incomparable elements $a, b \in \mathbb{Z}_n\}$. Then, \mathbb{Z}_n is a lattice if and only if every coset in $\{(\frac{n}{d}) + 1 \mid d \in S\}$ has smallest element.*

In the following theorem, we characterize the existence of $a \wedge b$ for $a, b \in \mathbb{Z}_n$.

Theorem 3.3. *Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i . Let $a, b \in \mathbb{Z}_n$ be incomparable and $d = \gcd(\gcd(a-1, b-1), n)$. Then, $a \wedge b$ exists if and only if the ideal $(\frac{n}{d})$ has the largest element.*

Proof. For each $i \in \{1, 2, \dots, k\}$, let $\beta_i, \gamma_i \in \mathbb{W}$ be the largest powers of prime p_i such that $a \equiv 1 \pmod{p_i^{\beta_i}}$ and $b \equiv 1 \pmod{p_i^{\gamma_i}}$ respectively. Let $f_i = \max\{(\alpha_i - \beta_i), (\alpha_i - \gamma_i), 0\}$ and $m = \prod_{i=1}^k p_i^{f_i}$. Then $m = \frac{n}{d}$. Let $c \in \mathbb{Z}_n$ and for each $i \in \{1, 2, \dots, k\}$, let $s_i \in \mathbb{N}$ be the largest powers of prime p_i such that $c \equiv 0 \pmod{p_i^{s_i}}$. Then, $c < a$ and $c < b$ if and only if $c(a-1) \equiv 0 \pmod{n}$ and $c(b-1) \equiv 0 \pmod{n}$ if and only if $s_i \geq (\alpha_i - \beta_i), (\alpha_i - \gamma_i)$ for all i if and only if $c \in (\frac{n}{d})$.

Suppose $a \wedge b$ exists. Since a and b are incomparable, we have $a \wedge b < a$ and $a \wedge b < b$. This yields $a \wedge b \in (\frac{n}{d})$. Let $x \in (\frac{n}{d})$. Then $x < a$ and $x < b$. Therefore $x < a \wedge b$. Thus $a \wedge b$ is the largest element of the ideal $(\frac{n}{d})$. Conversely, suppose that the ideal $(\frac{n}{d})$ has the largest element, say $e \in (\frac{n}{d})$. This yields $e < a$ and $e < b$. We claim that $a \wedge b = e$. Let $f \in \mathbb{Z}_n$ be such that $f < a$ and $f < b$. Then $f \in (\frac{n}{d})$. Therefore $f \leq e$. Thus $a \wedge b = e$. \square

From the proof of Theorem 3.3, it is clear that if $a \wedge b$ exists, then $a \wedge b$ is the largest element of the ideal $(\frac{n}{d})$. Also, if the ideal $(\frac{n}{d})$ has the largest element e , then $a \wedge b = e$.

The following corollary is an immediate consequence of Theorem 3.3.

Corollary 3.4. *Let $n \in \mathbb{N}$, $n > 1$ and $S' = \{d \in \mathbb{N} \mid d = \gcd(\gcd(a-1, b-1), n)\}$, for some incomparable elements $a, b \in \mathbb{Z}_n\}$. Then, \mathbb{Z}_n is a lattice if and only if every ideal in $\{(\frac{n}{d}) \mid d \in S'\}$ has largest element.*

Corollary 3.5. *Let $n \in \mathbb{N}$, $n > 1$, $S = \{d \in \mathbb{N} \mid d = \gcd(\gcd(a, b), n)\}$, for some incomparable elements $a, b \in \mathbb{Z}_n\}$ and $S' = \{d \in \mathbb{N} \mid d = \gcd(\gcd(a-1, b-1), n)\}$, for some incomparable elements $a, b \in \mathbb{Z}_n\}$. Then, every ideal in $\{(\frac{n}{d}) \mid d \in S'\}$ has largest element if and only if every coset in $\{(\frac{n}{d}) + 1 \mid d \in S\}$ has smallest element.*

Proof. Follows from Corollaries 3.2 and 3.4. \square

The following two lemmas relate the largest element of an ideal with the smallest element of a coset and vice versa.

Lemma 3.6. *Let $n = n_1 n_2$ with $n_1 \geq 1, n_2 \geq 3$ and $I = (n_1), J = (n_2)$. Then, the largest element of the ideal I becomes the smallest element of the coset $J + 1$.*

Proof. Since $|I| = n_2 \geq 3$, we have $n_1 \not\equiv -n_1 \pmod{n}$. Therefore n_1 and $-n_1$ are distinct elements in I . Let $e_1 n_1 \in I$ be the largest element of I . Then $x_1 n_1 \leq e_1 n_1$ for all $x_1 \in \mathbb{Z}$. This yields $n_1 \leq e_1 n_1$ and $-n_1 \leq e_1 n_1$. That is $n_1 \equiv e_1 n_1 \pmod{n}$ or $n_1 \equiv n_1 e_1 n_1 \pmod{n}$; and $-n_1 \equiv e_1 n_1 \pmod{n}$ or $-n_1 \equiv -n_1 e_1 n_1 \pmod{n}$. If $n_1 \equiv e_1 n_1 \pmod{n}$ and $-n_1 \equiv e_1 n_1 \pmod{n}$, then $n_1 \equiv -n_1 \pmod{n}$, a contradiction to the fact that $n_2 \geq 3$. Thus, either $n_1 \equiv n_1 e_1 n_1 \pmod{n}$ or $-n_1 \equiv -n_1 e_1 n_1 \pmod{n}$. Suppose $n_1 \equiv n_1 e_1 n_1 \pmod{n}$. That is $n_1(e_1 n_1 - 1) \equiv 0 \pmod{n_1 n_2}$. This implies that $e_1 n_1 - 1 \equiv 0 \pmod{n_2}$, hence $e_1 n_1 \in J + 1$. Similarly, $-n_1 \equiv -n_1 e_1 n_1 \pmod{n}$ implies that $e_1 n_1 \in J + 1$. Thus, in any case, $e_1 n_1 \in J + 1$. Let $y_2 n_2 + 1 \in J + 1$ be any element. Then $(y_2 n_2 + 1)e_1 n_1 = y_2 n_2 e_1 n_1 + e_1 n_1 \equiv e_1 n_1 \pmod{n}$. Thus $e_1 n_1$ is the smallest element of $J + 1$. \square

Lemma 3.7. *Let $n = n_1 n_2$ with $n_1 \geq 3, n_2 \geq 1$ and $I = (n_1), J = (n_2)$. Then the smallest element of the coset $J + 1$ becomes the largest element of the ideal I .*

Proof. Since $|J| = n_1 \geq 3$, we have $n_2 \not\equiv -n_2 \pmod{n}$. Therefore $n_2 + 1$ and $-n_2 + 1$ are distinct elements in the coset $J + 1$. Let $e_2 n_2 + 1 \in J + 1$ be the smallest element of $J + 1$. Then $e_2 n_2 + 1 \leq x_2 n_2 + 1$ for all $x_2 \in \mathbb{Z}$. This yields $e_2 n_2 + 1 \leq n_2 + 1$ and $e_2 n_2 + 1 \leq -n_2 + 1$. That is $e_2 n_2 + 1 \equiv n_2 + 1 \pmod{n}$ or $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(n_2 + 1) \pmod{n}$; and $e_2 n_2 + 1 \equiv -n_2 + 1 \pmod{n}$ or $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(-n_2 + 1) \pmod{n}$. If $e_2 n_2 + 1 \equiv n_2 + 1 \pmod{n}$ and $e_2 n_2 + 1 \equiv -n_2 + 1 \pmod{n}$, then $n_2 + 1 \equiv -n_2 + 1 \pmod{n}$, a contradiction to the fact that $n_1 \geq 3$. Thus, either $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(n_2 + 1) \pmod{n}$ or $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(-n_2 + 1) \pmod{n}$. Suppose $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(n_2 + 1) \pmod{n}$. That is $(e_2 n_2 + 1)(n_2) \equiv 0 \pmod{n_1 n_2}$. This implies that $e_2 n_2 + 1 \equiv 0 \pmod{n_1}$, hence $e_2 n_2 + 1 \in I$. Similarly, $e_2 n_2 + 1 \equiv (e_2 n_2 + 1)(-n_2 + 1) \pmod{n}$ implies that $e_2 n_2 + 1 \in I$. Thus, in any case, $e_2 n_2 + 1 \in I$. Let $y_1 n_1 \in I$ be any element. Then $(y_1 n_1)(e_2 n_2 + 1) = y_1 n_1 e_2 n_2 + y_1 n_1 \equiv y_1 n_1 \pmod{n}$. Thus $e_2 n_2 + 1$ is the largest element of I . \square

Remark 3.8. Let $a \in GP(\mathbb{Z}_n)$ and I be the ideal generated by a . Then a_u is the largest element of I . For $ma \in I$, $maa_u = ma$, hence $ma \leq a_u$.

If $a, b \in GP(\mathbb{Z}_n)$ then $a \vee b$ and $a \wedge b$ both exists in the poset $GP(\mathbb{Z}_n)$ (see [1]). The following two theorems gives the existence of $a \vee b$ and $a \wedge b$ in the poset \mathbb{Z}_n where $a, b \in GP(\mathbb{Z}_n)$.

Theorem 3.9. *If $a, b \in GP(\mathbb{Z}_n)$ then $a \vee b$ exists in the poset \mathbb{Z}_n . Further, $a \vee b \in GP(\mathbb{Z}_n)$.*

Proof. If a and b are comparable then clearly $a \vee b$ exists and $a \vee b \in GP(\mathbb{Z}_n)$. Suppose a and b are incomparable. Let $d = \gcd(\gcd(a, b), n)$, I be the ideal generated by d and J be the ideal generated by $\frac{n}{d}$. As, $a, b \in GP(\mathbb{Z}_n)$, by Remark 1.2(iii), $\gcd(a, b) \in GP(\mathbb{Z}_n)$. Therefore $d \in GP(\mathbb{Z}_n)$. By Remark 3.8, the ideal I possesses the largest element, say e and $e \in GP(\mathbb{Z}_n)$. Since $d|a$ and $d|b$, we have $a, b \in I$. As, a and b are incomparable, we have $|I| = \frac{n}{d} \geq 3$. By Lemma 3.6, e becomes the smallest element of the coset $J + 1$. By Theorem 3.1, $a \vee b$ exists and $a \vee b = e$. Thus, $a \vee b = e \in GP(\mathbb{Z}_n)$. \square

Theorem 3.10. *Let $a, b \in GP(\mathbb{Z}_n)$ be such that $a - 1, b - 1 \in GP(\mathbb{Z}_n)$. Then $a \wedge b$ exists in the poset \mathbb{Z}_n and $a \wedge b \in GP(\mathbb{Z}_n)$.*

Proof. If a and b are comparable then clearly $a \wedge b$ exists and $a \wedge b \in GP(\mathbb{Z}_n)$. Suppose a and b are incomparable. Let $d = \gcd(\gcd(a - 1, b - 1), n)$ and I be the ideal generated by $\frac{n}{d}$. As, $a - 1, b - 1 \in GP(\mathbb{Z}_n)$, by Remark 1.2(iii), $\gcd(a - 1, b - 1) \in GP(\mathbb{Z}_n)$. Therefore $d \in GP(\mathbb{Z}_n)$, and hence $\frac{n}{d} \in GP(\mathbb{Z}_n)$. By Remark 3.8, the ideal I possesses the largest element, say e and $e \in GP(\mathbb{Z}_n)$. By Theorem 3.3, $a \wedge b$ exists and $a \wedge b = e$. Thus $a \wedge b = e \in GP(\mathbb{Z}_n)$. \square

In the following theorem, we give a necessary and sufficient condition for the poset \mathbb{Z}_n to be a lattice.

Theorem 3.11. *Let $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$ with $\alpha_i > 0$, for all i . Then, \mathbb{Z}_n is a lattice if and only if for every $n_1 \geq 3$ with $n = n_1 n_2$, (n_1) possess the largest element.*

Proof. Suppose \mathbb{Z}_n is a lattice. Let $n = n_1 n_2$ with $n_1 \geq 3$. If (n_1) does not possess the largest element, then $|(n_1)| = n_2 \geq 3$. Let $a = n_1$; and $b = pn_1$, where p is a prime such that $\gcd(p, n_2) = 1$ and $n_2 \nmid (p - 1)$. Then $a, b \not\equiv 0 \pmod{n}$ and $a \not\equiv b \pmod{n}$. If $a < b$, then $a \equiv ab \pmod{n}$. That is $n_1 \equiv n_1 pn_1 \pmod{n}$. This yields $n_1(pn_1 - 1) \equiv 0 \pmod{n}$. This implies that $pn_1 \equiv 1 \pmod{n_2}$. Hence $\gcd(n_1, n_2) = 1$. Consequently $n_1 \in GP(\mathbb{Z}_n)$. By Remark 3.8, (n_1) possess the largest element, a contradiction. Therefore $a \not\leq b$. Similarly, $b \not\leq a$. Thus a and b are incomparable. Observe that $\gcd(\gcd(a, b), n) = n_1$. As, $(\frac{n}{n_2}) = (n_1)$ does not possess the largest element. By Lemma 3.7, the coset $(n_2) + 1$ does not possess the smallest element. By Corollary 3.2, \mathbb{Z}_n is not a lattice, a contradiction. Therefore (n_1) possess the largest element. Conversely, suppose for every $n_1 \geq 3$ with $n = n_1 n_2$, (n_1) possess the largest element. If \mathbb{Z}_n is not a lattice, then by Corollary 3.2, there exists incomparable elements $a', b' \in \mathbb{Z}_n$ such that $d' = \gcd(\gcd(a', b'), n)$ and $(\frac{n}{d'}) + 1$ does not possess the smallest element. Therefore $\frac{n}{d'} = |(d')| \geq 3$ and $|(\frac{n}{d'}) + 1| \geq 3$. Hence $|(\frac{n}{d'})| = d' \geq 3$. Let $n'_1 = d'$ and $n'_2 = \frac{n}{d'}$. Then $n'_1 \geq 3$ and $n = n'_1 n'_2$. By Lemma 3.6, (n'_1) does not possess the largest element, a contradiction. Thus \mathbb{Z}_n is a lattice. \square

Remark 3.12. Let $a \in N(\mathbb{Z}_n) \setminus \{0\}$. If $b \in \mathbb{Z}_n$ be such that $b < a$ then $b = ba = ba^m$ for any $m \in \mathbb{N}$. Since $a \in N(\mathbb{Z}_n)$, we have $b = 0$. Hence $a_l = 0$. From this, it follows that, if I is an ideal generated by a nilpotent element of \mathbb{Z}_n such that $|I| \geq 3$, then I does not possess the largest element. Thus \mathbb{Z}_n is not a lattice.

REFERENCES

- [1] Anil Khairnar and B. N. Waphare, *Order properties of generalized projections*, Linear and Multilinear Algebra (2016), DOI:10.1080/03081087.2016.1242554.
- [2] László Tóth, *Regular integers modulo n* , Annales Univ. Sci. Budapest., Comp., **29** (2008), 263-275.

◆◆◆

Department of Mathematics, Abasaheb Garware College, Pune-411004, India.
E-mail address: anil.khairnar@mesagc.org; anil.maths2004@yahoo.com

Center for Advanced Studies in Mathematics, Department of Mathematics, Savitribai Phule Pune University, Pune-411007, India.

E-mail address: bnwaph@math.unipune.ac.in; waphare@yahoo.com